Attorney's Docket No.: 10559-755001/P13653
Intel Corporation

REMARKS

Claims 1-33 are pending, with claims 1, 13, 22, 24, 26, and 31 being independent. New claims 34-35 have been added. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Allowed and Allowable Claims:

Claims 13-21, 26-27, and 31-33 are indicated as allowed. Additionally, claims 28-30 should be allowed, at least based on their dependence from an allowed base claim. It is noted that claims 28-30 are not actually addressed in the Final Office Action mailed November 15, 2005. Thus, presumably, the identification of allowed claims in paragraph 22 of the Final Office Action includes a typographical error, in that, claims 28-30 are in fact allowed based on the current record. In support of this conclusion, please note that claim 30 includes the same language as claim 12, which has been indicated as allowable based on this language.

Claims 11 and 12 are objected to as being dependent upon a rejected base claim. The claims are retained.

Interview Summary:

Examiners Perungavoor and Barron are thanked for the interview, which was conducted with Applicants' representative, Mr. Hunter, on January 11, 2006. During the interview, claims 5, 8, 9, 10 and 25, and the Markham reference (U.S. Patent Publication 2003/0126468 A1) were discussed. Agreement was reached that: (1) the current rejections of claims 5 and 25 are improper, and these claims are in fact allowable in view of the allowance of claim 31; (2) the current rejection of claim 8 is not supported by the cited portion of Markham, and this rejection should be withdrawn as currently written in the Final Office Action; (3) the current rejection of claim 9 is not supported by the cited portion of Markham, and this rejection should be withdrawn as currently written in the Final Office Action; and (4) the rejection of claim 10 fails to address the actual language of claim 10, and this rejection should be withdrawn as currently written in the Final Office Action.

In addition, Examiner Perungavoor indicated during the interview that there is an error in paragraph 2 of the Final Office Action with respect to the reasons for allowance of independent claims 13 and 26. The Final Office Action states in paragraph 2 that Applicant's prior arguments are persuasive, but then goes on to identify a feature from the specification as the

reason for allowance of claims 13 and 26. However, this feature from the specification is not in fact recited in either claim 13 or claim 26. This feature has been added to new claims 34 and 35, which depend from claims 13 and 26, respectively. Thus, new claims 34 and 35 should be allowable.

Furthermore, independent claims 13 and 26 recite, "initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests." (Emphasis added.) Markham does not describe application-specific intrusion signatures, nor using such in response to one or more unauthorized requests for network communication services from an invoked application. The arguments presented in the prior response with respect to these features of claims 13 and 26 are not addressed in the Final Office Action. Additionally, when discussing claim 8 (which also recites "an application-specific intrusion signature") during the interview, Examiners Perungavoor and Barron could not identify where in Markham an application-specific intrusion signature is described. Thus, claims 13-21 and 26-33 should remain allowed.

Claim Rejections:

Claims 1-10 and 22-25 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by Markham (U.S. Patent Publication 2003/0126468 A1) with priority under 35 U.S.C. § 119(a) based on PCT No. PCT/US01/17153. This contention is respectfully traversed.

Markham is directed to "a system and method of enforcing a security policy by distributing aspects of the security policy across a number of devices while retaining the ability to react to attacks and to changes in the computing environment." (*See* Markham at ¶ 10.) Markham describes distribution of firewall functionality to independent components of host systems in a network, and providing centralized management of the distributed firewall integrated with autonomic response systems. (*See* Markham at ¶ 35.)

The present application describes integrating firewall functionality with intrusion detection on end nodes in a network using application-specific network policies. (*See* Specification at ¶s 21-22 and 25-26.) This enables increased specificity with respect to designating authorized network communications, and can result in significantly improved network intrusion detection, e.g., an application-specific network policy can be used to track application behavior and

identify abnormal behavior specific to one application. (*See* Specification at ¶ 38.)

Independent claim 1 recites, "receiving requests for network communication services from an invoked application; selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy; and monitoring inbound network communications, based on the authorized requests, to detect an intrusion." (Emphasis added.) Markham fails to teach or suggest application-specific network policies, or use of such in selectively designating requests for network communication services from an invoked application as authorized or unauthorized.

In response to the prior arguments presented regarding this claimed subject matter, the Final Office Action cites paragraph 76 of Markham, which reads:

> The per-host nature of the distributed firewall allows the policy to be easily tuned to the needs of a specific host. For example, if no one should be Telneting to your web server, the NIC 14 associated with that web server can be configured to block both incoming and outgoing Telnet (from both inside and outside the organization).

However, the way the NIC 14 does this in Markham is by looking at the port number associated with the communication. (*See*

e.g., Markham at ¶s 78, 100, 133, and 154.) A rogue application can use the port associated with Telnet, and Markham will treat this application as though it were Telnet. Thus, Markham cannot accurately distinguish between different applications.

Markham describes a network firewall concept in which a source application is assumed based on the port associated with the packets being inspected. Thus, network policies in Markham may be port-specific, but they are not in fact application-specific, as claimed. For at least these reasons, independent claim 1 should be in condition for allowance.

Independent claims 13, 22, 24, and 26 cover subject matter that also includes use of an application-specific network policy. Thus, for at least the above reasons, independent claims 13, 22, 24, and 26 should be in condition for allowance.

Dependent claims 2-12, 14-21, 23-25, and 27-30 should be patentable based on the above arguments and the additional recitations they contain.

For example, claim 2 recites, "blocking the inbound network communications that fail to correspond to an authorized request; and monitoring the blocked inbound network communications to detect an intrusion." (Emphasis added.)

Markham describes use of intrusion detection, including doing intrusion detection management at a master device (LSS 20) and doing intrusion detection at an end node (NIC 14). (*See* Markham at ¶s 36 and 45.) However, Markham does not describe designating a request for communication services from an invoked application as authorized or unauthorized, blocking inbound communications that fail to correspond to an authorized request, and monitoring the blocked inbound communications to detect an intrusion.

The cited portion of Markham (¶s 36 and 94-100) clearly describe redirection of traffic to LSS (local security server) 20 for filtering, and this redirection is done either (a) "for authentication only during connection setup", or (b) "for the duration of the session (i.e., for doing things like virus scanning)." (*See* Markham at ¶ 94.) Neither of these embodiments, describes blocking inbound communications that fail to correspond to an authorized request, and monitoring the blocked inbound communications to detect an intrusion. This subject matter of claim 2 can result in a significant reduction in the overall amount of network traffic that needs to be monitored to detect intrusions. (*See* Specification at ¶ 20.) Claim 2 (and claims 13, 26 and 32, which include similar

features) should be allowable for at least these additional reasons.

Claim 3 recites, "examining the blocked inbound network communications to detect an intrusion prelude; identifying a source for a detected intrusion prelude; and initiating monitoring of inbound network communications from the identified source." (Emphasis added.) An "intrusion prelude" is defined in the present specification as "communication activities that typically precede an intrusion." (*See* Specification at ¶ 19.) Markham does not address intrusion preludes, nor does Markham describe responding to a detected intrusion prelude by identifying a source and initiating monitoring of inbound network communications from that identified source.

The cited portion of Markham describe blocking of all traffic for a compromised host and prevention of address spoofing. (See Markham at ¶s 32 and 34.) Markham neither teaches nor suggests detecting an intrusion prelude and then singling out a source of that intrusion prelude for greater scrutiny. Furthermore, the Final Office Action fails to address these previously presented arguments. (*See* ¶ 3 of the Final Office Action.) Thus, claim 3 (and claims 14, 27 and

33, which include similar features) should be allowable for at least these additional reasons.

Claims 5, 17, and 25 should also be allowable in view of the allowance of claim 31.

Claims 7 and 8 should also be allowable in view of the arguments presented above in connection with claims 13 and 26.

Furthermore, claim 9 should be allowable because Markham does not describe identifying an invoked application by examining a set of instructions embodying the invoked application. The cited portion of Markham say nothing about examining application instructions to identify an invoked application, as agreed in the interview. Thus, claim 9 (and claims 15 and 28, which include similar features) should be allowable for at least these additional reasons.

Claim 10 should be allowable because Markham does not describe monitoring network communications for an invoked application in an intrusion detection system component invoked with the invoked application. The cited portion of Markham do not support the current rejection of claim 10, as agreed in the interview. Thus, claim 10 (and claim 20) should be allowable for at least these additional reasons.

Finally, claim 21 should be allowable for reasons similar to claim 11, and claims 19 and 30 should be allowable for reasons similar to claim 12.

Conclusion

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

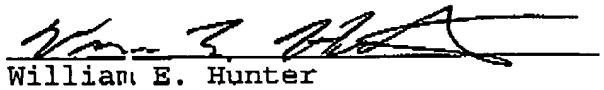
It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art teaches or suggests the features which are claimed, and therefore that all of these claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

Attorney's Docket No.: 10559-755001/P13653
Intel Corporation

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: January 13, 2006



William E. Hunter
Reg. No. 47,671
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10577321.doc